

HOGYAN KÉSZÜLJÜNK FEL AZ ÚJ JOGSZABÁLYI KÖVETELMÉNYEKRE?

Napjainkban minden szervezet üzleti érdeke, hogy a kiberbiztonsággal foglalkozzon és minimalizálja az információ-biztonsági kockázatokat. Emellett egyre több, erre vonatkozó külső elvárás jelenik meg, mint például a **NIS2** irányelv, a **Kibertan.tv** (2023. évi XXIII. törvény) vagy a **DORA** rendelet. A megjelent rendeletek és jogszabályok az új információ-biztonsági követelmények és feladatok mellett szigorú határidőket is előírnak az érintett szervezeteknek – érdemes időben felkészülni! Kiadványunkban bemutatott szolgáltatásaink ezt hivatottak segíteni.

SZÁMÍTHAT RÁNK A TELJES FOLYAMAT SORÁN!



A FELKÉSZÜLÉS LÉPÉSEI

1 AZONOSÍTÁS

Első lépés a jogszabály általi érintettség azonosítása, majd amennyiben releváns, a regisztrációs adatok megküldése az érintett hatóság számára (pl. Kibertan.tv esetében SZTFH részére).



Ezt követően az érintett elektronikus információs rendszereket a jogszabály által meghatározottak szerint biztonsági osztályba kell sorolni, mely meghatározza a szervezetre, valamint a rendszerekre vonatkozó információbiztonsági követelményeket.

2 KÖVETELMÉNYEK AZONOSÍTÁSA



Az előző pontban azonosított követelményeknek való megfelelést egy compliance audit lefolytatása során ellenőrizhetjük, melynek eredményeként a feltárt hiányosságokra, eltérésekre akciótervet kell készíteni.

3 MEGFELELÉS VIZSGÁLATA



A hiányosságok és nemmegfelelések kezelésére irányuló akciótervek végrehajtásával tervezetten vezethetők be a szükséges javító intézkedések, hiányzó kontrollok.

4 MEGFELELÉS BIZTOSÍTÁSA



Utolsó lépés a külső, akkreditált fél általi tanúsítás végrehajtása, vagy amennyiben lehetőség van rá, önértékelés alapján megfelelési nyilatkozat kiállítása és benyújtása az érintett hatóságnak.

5 MEGFELELŐSÉG ÉRTÉKELÉS, TANUSÍTÁS



SZOLGÁLTATÁSAINK



Információbiztonsági felelős



Szabályzat készítés



Compliance, audit



Képzés, oktatás



Biztonságtudatosság



Üzleti hatás-elemzés, BIA



Kockázatmenedzsment



Üzletfolytonosságmenedzsment



Etikus hackelés





INFORMÁCIÓBIZTONSÁGI FELELŐS SZOLGÁLTATÁS (IBF)

Olyan képesítéssel rendelkező személy kirendelése, aki a szervezetnél a jogszabályi követelmények megfeleltetésével, a törvény által előírtak támogatásával foglalkozik.



SZABÁLYZATKÉSZÍTÉS ÉS FELÜLVIZSGÁLAT

Külső követelményeknek (például jogszabályok, szabványok) megfelelő, a szervezet méretéhez és jellegéhez igazodó információbiztonsági szabályozási környezet kialakítása, karbantartása és felülvizsgálata.



SZAKÉRTŐI KÉPZÉSEK

Szakértőknek szóló képzéseink kockázatmenedzsment, üzletfolytonosság-menedzsment, SocialEngineering és biztonság tudatosság, valamint gamifikáció témában.



BIZTONSÁGTUDATOSSÁGI OKTATÁS

SocialEngineering audit, hagyományos oktatások, valamint újszerű gamifikációs megoldások, mint például szabadulószoza, társasjáték, online Awareness Game.



FELMÉRÉSEK

Adatvagyon-, folyamat- és erőforrás-felmérések elvégzése és tanácsadói támogatás biztosítása.



ÜZLETI HATÁSELEMZÉS (BIA)

Üzleti hatáselemzés készítése, kritikus folyamatok és támogató erőforrások azonosítása.



KOCKÁZATMENEDZSMENT

Kockázatelemzés készítése, kockázatarányos védelmi intézkedés javaslatok kidolgozása, meghatározása és azok megvalósítása, kockázatkezelés támogatása.



ÜZLETFOLYTONOSSÁG-MENEDZSMENT

Üzletfolytonosság-menedzsment rendszer bevezetése, szabályozók kialakítása és karbantartása. Üzletfolytonossági akciótervek (BCP) és erőforrás-helyreállítási akciótervek (DRP) készítése és tesztelése.



COMPLIANCE AUDIT

A szervezetre vonatkozó jogszabályoknak és más külső követelményeknek (például IBTV, MNB ajánlások, NIS2, Kibertan.tv, DORA rendelet, ISO 27001) való megfelelés felmérése, hiányosságok és nem-megfelelések kezelésének biztosítása, felkészülés támogatása.



ETIKUS HACKELÉS

Sérülékenységvizsgálatok (infrastruktúra- és alkalmazás vizsgálatok) elvégzése, hibajavítások, technológiai tanácsadás és fejlesztések biztonsági támogatása.



SECURITY INVENTORY AND RISK EVALUATION NETWORK

Saját fejlesztésű SIREN rendszerünk komplex megoldást nyújt a szervezeteknek az üzleti folyamatok, erőforrások, illetve az adatvagyon felmérésére, üzleti hatáselemzés és különböző módszertanú kockázatelemzések készítésére, sőt a kockázatkezelő intézkedések nyomon követésére és az üzletfolytonosság-menedzsment feladatok támogatására.

